

OpenSSL FIPS Cryptographic Module by Open Source Software Institute

Reference Material
April 28, 2003

Cryptographic Module Validation Program FIPS 140-1 and FIPS 140-2 Pre-validation List

<http://csrc.nist.gov/cryptval/preval.htm>

Security Requirements for Cryptographic Modules

FIPS 140-2 - Federal Information Processing Standard Publication

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

The FIPS 140-2 standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive, but unclassified, information.

The Cryptographic Module Validation Program (CMV) validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-2 and other cryptography-based standards. The CMVP is a joint effort between the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada).

NIST (www.nist.gov) is part of the U.S. Department of Commerce

OpenSSL Project

<http://www.openssl.org>

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and [Open Source](#) toolkit implementing the [Secure Sockets Layer](#) (SSL v2/v3) and [Transport Layer Security](#) (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.